Exfiltration of Data from Secure Environments Using Fiber-Like Nano-Robotic Drone Swarms in Conjunction with BDCNN Exfiltration Networks (ibid.)

7 September 2023
Simon Edwards
Research Acceleration Initiative

Introduction

The most critical and secure computer systems are often air-gapped and they are sometimes even hermetically sealed. Although air filters would capture nanofiber-based nanobots, these fibers may be carried into secure areas unwittingly by authorized personnel on their clothing.

Abstract

Once inside, such nanobots could find their way into mainframe computers. A recently conceptualized technology called Bruteforced Directional Calibration in search of Nearest Neighbor (BDCNN) can facilitate active data exfiltration from contested environments and with this advancement, nanoscopic sensors may be made to "float" into data centers, come to rest upon the physical CPU itself and use this extreme proximity to detect internal activity within the processor (or, more likely, the data pipelines leading to and from the processor) and relay the detected signals using collimated microwave energy and a series of hundreds or thousands of nanoscopic nodes to get the data out of the secure facilities and to a larger urban network and from there, to a collimated microwave beam-facilitated satellite uplink.

Upon the completion of a data exfiltration mission, to prevent the detection and reverse-engineering of the technology that makes this possible, another recently proposed technology called an Electrically-Controlled Variable Acidity Plastic (ECVAP) (ibid.) can be used to trigger the self-destruction of the nanobots through a pseudo-acidification process that would prevent analysis of the bots if their remnants were ever discovered.

Conclusion

The plausibility of such a data exfiltration approach demonstrates how even the most recently conceptualized technologies may augment one another and lead to further innovation.